UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,719	09/08/2006	Agostinho De Arruda Villela	2171323-000002	9289

44777 7590 04/28/2011
W. EDWARD RAMAGE
COMMERCE CENTER SUITE 1000
211 COMMERCE ST
NASHVILLE, TN 37201

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/28/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eramage@bakerdonelson.com

Office Action Summary	Application No.	Applicant(s)	
	10/598,719	DE ARRUDA VILLELA, AGOSTINHO	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/4/2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

\DETAILED ACTION

In view Appellant's Appeal Arguments filed 6/14/2010, PROSECUTION IS HEREBY REOPENED. A new ground(s) of rejection cited under prior art references Moshir, Aissi, Cravo De Almeida Hyman, Cui and Abburi are set forth below. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final)or a reply under 37 CFR 1.113 (if this Office action is final); or,(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below. Claims 17-35 are pending.

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2468

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 17-19, 22, 23, 26-28 and 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir (US Patent Publication 2004/0003266) in view of Aissi et al. (US Patent Publication No. 2005/0149730 and Aissi hereinafter) in view of Cravo De Almeida et al. (US Patent Publication No. 2003/0055931 and Almeida hereinafter).

2. As per claim 17: Moshir discloses a method for identifying devices and controlling access to a service, comprising the steps of (see abstract): sending the digital signature of the device to an authentication server (Paragraph 109, signature information sent to the updated server).

determining whether the device has been excluded from accessing or enrolling in the service (i.e., ... the Examiner notes that applicant states in paragraph 9 of applicant's original disclosure that the term "service" relates to access to an Internet page, an Intranet page, or any other type of computer server or computer-based service. The Examiner contends that Moshir discloses in paragraph 81 an enrollment process for indicating a desired level of participation. A preferred embodiment of the invention has three different user levels: guest, regular, and executive. A guest is allowed to view a web site. The Examiner adds that all participation is through a user's target computer (e.g., device) and that it is understood that participation depends on the user and the target computer was enrolled, and that access permission to web sites (e.g., computer based services) would be control accordingly);

Moshiri's teachings do not expressly teach:

generating a digital signature for the device by hashing the software and hardware configuration data. In this instance the Examiner notes the teachings of Aissi paragraph 58 & figure 7A, where Aissi discloses platform configuration may be a hash. Therefore given the system described above by Moshiri, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance data security by employing Aissi's ability to hash device configuration data.

The system of Moshiri and Aissi do not expressly teach:

collecting data related to software and hardware configurations from a device through a software agent; In this instance the Examiner notes the teachings of Almeida paragraph 27, where Almeida discloses device configuration utilizing a software agent (e.g., plug-in). Therefore given the system described above by Moshiri and Aissi, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance device authentication by employing Almeida's capability to collect device configuration data utilizing a software agent.

3. As per claim 18: Moshir discloses where the digital signature sent to the authentication server is encrypted (see Moshir, Paragraph 1{)9, signature may also be encrypted).

4. As per claim 19: Moshir discloses where the software agent is installed on the device as part of the process of using the device to access a service (see Moshir, Paragraph 23; discover agent is installed on the hardware and software of the target computer).

5. As per claim 22: Moshir discloses where the authentication server compares the digital signature sent with one or more previously- stored digital signatures (See Moshir, Paragraph 91, discloses comparing previous information (i.e. signature) stored in library).

6. As per claim 23: Moshir discloses the method where the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service (See Moshir, Paragraph 24; update server 528 can present the user with detailed reports of the current patch status for all computers within the network).

7. As per claim 26: Moshir discloses the method where the authentication server allows minor modifications to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device (See Moshir, Paragraph 99; discloses hardware information including specific software updates with configurations).

8. As per claim 27: Moshir discloses the method where the previously-stored digital signature of the device is updated to reflect the modifications (See Moshir, Paragraph 109, 185; signature updates).

9. As per claim 28: Moshir discloses the method where the authentication server logs all accesses or attempted accesses by a device to the service (See Moshir, Paragraph 61; the update server can drill through the firewall to access the target computer).

10. As per claims 31 and 35: Moshir discloses a method for identifying devices and controlling access to a service, comprising the steps of (see abstract): sending the digital signature of the device to an authentication server (Paragraph 109, signature information sent to the updated server).

determining whether the device has been excluded from accessing or enrolling in the service (i.e., ... the Examiner notes that applicant states in paragraph 9 of applicant's original disclosure that the term "service" relates to access to an Internet page, an Intranet page, or any other type of computer server or computer-based service. The Examiner contends that Moshir discloses in paragraph 81 an enrollment process for indicating a desired level of participation. A preferred embodiment of the invention has three different user levels: guest, regular, and executive. A guest is allowed to view a web site. The Examiner adds that all participation is through a user's

target computer (e.g., device) and that it is understood that participation depends on the user and the target computer was enrolled, and that access permission to web sites (e.g., computer based services) would be control accordingly);

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero and registering the device as authorized to access the service (i.e., the Examiner notes applicant usage of the term "or" renders the claims in alternative form. As such with regards to applicant's claim limitation: "verifying that the device is not on a list or in a group of devices not allowed to access the service", the Examiner notes Moshir, Paragraph 24; update sewer 528 can present the user with detailed reports of the current patch status for all computers within the network).

Moshiri's teachings do not expressly teach:

generating a digital signature for the device by hashing the software and hardware configuration data. In this instance the Examiner notes the teachings of Aissi paragraph 58 & figure 7A, where Aissi discloses platform configuration may be a hash. Therefore given the system described above by Moshiri, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance data security by employing Aissi's ability to hash device configuration data.

The system of Moshiri and Aissi do not expressly teach:

collecting data related to software and hardware configurations from a device through a software agent; In this instance the Examiner notes the teachings of Almeida paragraph 27, where Almeida discloses device configuration utilizing a software agent (e.g., plug-in). Therefore given the system described above by Moshiri and Aissi, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance device authentication by employing Almeida's capability to collect device configuration data utilizing a software agent.

11. Claim 32, Moshir method of claim 31, further comprising the step of verifying the identity of the device each time it subsequently attempts to access the service (i.e., ... the Examiner notes that applicant states in paragraph 9 of applicant's original disclosure that the term "service" relates to access to an Internet page, an Intranet page, or any other type of computer server or computer-based service. The Examiner contends that Moshir discloses in paragraph 81 an enrollment process for indicating a desired level of participation. A preferred embodiment of the invention has three different user levels: guest, regular, and executive. A guest is allowed to view a web site. The Examiner adds that all participation is through a user's target computer (e.g., device) and that it is understood that the depending on how the user and target computer was enrolled, that access permission to web sites (e.g., computer based services) would be control accordingly).

12. As per claim 33: Moshir discloses a method for identifying devices and controlling access to a service, comprising the steps of (see abstract): sending the digital signature of the device to an authentication server (Paragraph 109, signature information sent to the updated server).

comparing the digital signature sent with one or more previously-stored digital signatures for the device (i.e., ...teaches a comparing previous information (i.e. signature) stored in library) [par. 91]).

Moshiri's teachings do not expressly teach:

generating a digital signature for the device by hashing the software and hardware configuration data. In this instance the Examiner notes the teachings of Aissi paragraph 58 & figure 7A, where Aissi discloses platform configuration may be a hash. Therefore given the system described above by Moshiri, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance data security by employing Aissi's ability to hash device configuration data.

The system of Moshiri and Aissi do not expressly teach:

collecting data related to software and hardware configurations from a device through a software agent; In this instance the Examiner notes the teachings of Almeida paragraph 27, where Almeida discloses device configuration utilizing a software agent (e.g., plug-in). Therefore given the system described above by Moshiri and Aissi, a person of ordinary skill in the art would have recognized advantage of modifying the

system to enhance device authentication by employing Almeida's capability to collect device configuration data utilizing a software agent.

13. As per claim 34: Moshir discloses a method for identifying devices and controlling access to a service, comprising the steps of (see abstract): sending the digital signature of the device to an authentication server (Paragraph 109, signature information sent to the updated server).

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero and registering the device as authorized to access the service (i.e., the Examiner notes applicant usage of the term "or" renders the claims in alternative form. As such with regards to applicant's claim limitation: "verifying that the device is not on a list or in a group of devices not allowed to access the service", the Examiner notes Moshir, Paragraph 24; update sewer 528 can present the user with detailed reports of the current patch status for all computers within the network).

Moshiri's teachings do not expressly teach:

generating a digital signature for the device by hashing the software and hardware configuration data. In this instance the Examiner notes the teachings of Aissi paragraph 58 & figure 7A, where Aissi discloses platform configuration may be a hash. Therefore given the system described above by Moshiri, a person of ordinary skill in the

art would have recognized advantage of modifying the system to enhance data security by employing Aissi's ability to hash device configuration data.

The system of Moshiri and Aissi do not expressly teach:

collecting data related to software and hardware configurations from a device through a software agent; In this instance the Examiner notes the teachings of Almeida paragraph 27, where Almeida discloses device configuration utilizing a software agent (e.g., plug-in). Therefore given the system described above by Moshiri and Aissi, a person of ordinary skill in the art would have recognized advantage of modifying the system to enhance device authentication by employing Almeida's capability to collect device configuration data utilizing a software agent.

14. Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir and Aissi in view of Almeida as applied to claim 17 above, and further in view of Cui (US Patent Publication 2005/0166053).

15. As per claim 20: Moshir and Aissi in view of Almeida discloses the method where the digital signature sent to the authentication server is encrypted (See Moshir; Paragraph 109, signature information sent to the updated server). Moshir and Aissi in view of Almeida doesn't specifically disclose wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed. Cui discloses a determination is made whether the device

signature(s) are to be rolled over; updating (rolling) the device signature(s) is based, in part, on a pre\- determined period of time (Paragraph 63, 70). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Moshir and Aissi in view of Almeida 's wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed, as taught by Cui. The motivation would have been to provide an improved digital signature generation process.

16. As per claim 21: Moshir and Aissi in view of Almeida discloses the method where the digital signature sent to the authentication server is encrypted (See Moshir; Paragraph 109, signature information sent to the updated server). Moshir and Aissi in view of Almeida doesn't specifically disclose wherein the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device. Cui discloses determining at least one device signature for a mobile device (See fig. 3; Paragraph 51, 52). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Moshir and Aissi in view of Almeida 's wherein the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device, and the hashes cannot be reversed, as taught by Cui. The motivation would have been to provide an improved digital signature generation process.

17. Claims 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir and Aissi in view of Almeida as applied to claim 17 above, and further in view Abburi (US Patent Publication 2003/0084306).

18. As per claim 24: Moshir and Aissi in view of Almeida discloses the method of claim 6, sending the digital signature of the device to an authentication server sending the digital signature of the device to an authentication server (See Moshir, Paragraph 109, signature information sent to the updated server). Moshir and Aissi in view of Almeida doesn't specifically disclose wherein the authentication server allows a maximum number of enrollments for a particular device. Abburi discloses the maximum number of devices had been enrolled and device 1302f will be added to device store 1522 on synchronization server 1402 (Paragraph 464, 471). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Moshir and Aissi in view of Almeida 's wherein the authentication server allows a maximum number of enrollments for a particular device, as taught by Abburi. The motivation would have been to provide an improved digital signature generation process.

19. As per claim 25: Moshir and Aissi in view of Almeida and further view of Abburi discloses the method of claim 24, wherein the maximum number of enrollments is zero (See Abburi, Paragraph 464, 471).

20. Claims 29 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir and Aissi in view of Almeida as applied to claim 17 above, and further in view Hyman (US Patent 7,117,528).

21. As per claim 29: Moshir and Aissi in view of Almeida discloses the method of claim 17, sending the digital signature of the device to an authentication server sending the digital signature of the device to an authentication server (See Moshir, Paragraph 109, signature information sent to the updated server). Moshir and Aissi in view of Almeida doesn't specifically disclose wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy. Hyman discloses users of the client computers register with the authentication server for generating user account (See fig 2; Col 7 lines 14-27; e.g. multiple devices can be registered for a single user with the authentication server). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Moshir and Aissi in view of Almeida's wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy, as taught by Hyman. The motivation would have been to provide an improved digital signature generation process.

22. As per claim 30: Moshir and Aissi in view of Almeida in further view of Hyman discloses the method of claim 29, wherein a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier

than the device to be unregistered (See Hyman, Col 10, lines 3-6; the new account is created and the old account is put into a ForceRename state).

23. Claims 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moshir in view of Aissi and further in view of Almeida

Response to Arguments

Applicant's arguments with respect to claims 17-35 have been considered but are moot in view of the new ground(s) of rejection. The Examiner notes for the record that the combination of Moshiri, Aissi and Almeida, specifically Almeida affords the capability to collect device configuration data utilizing a software agent (e.g., plug-in).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2468